Bundesministerium
des Innern

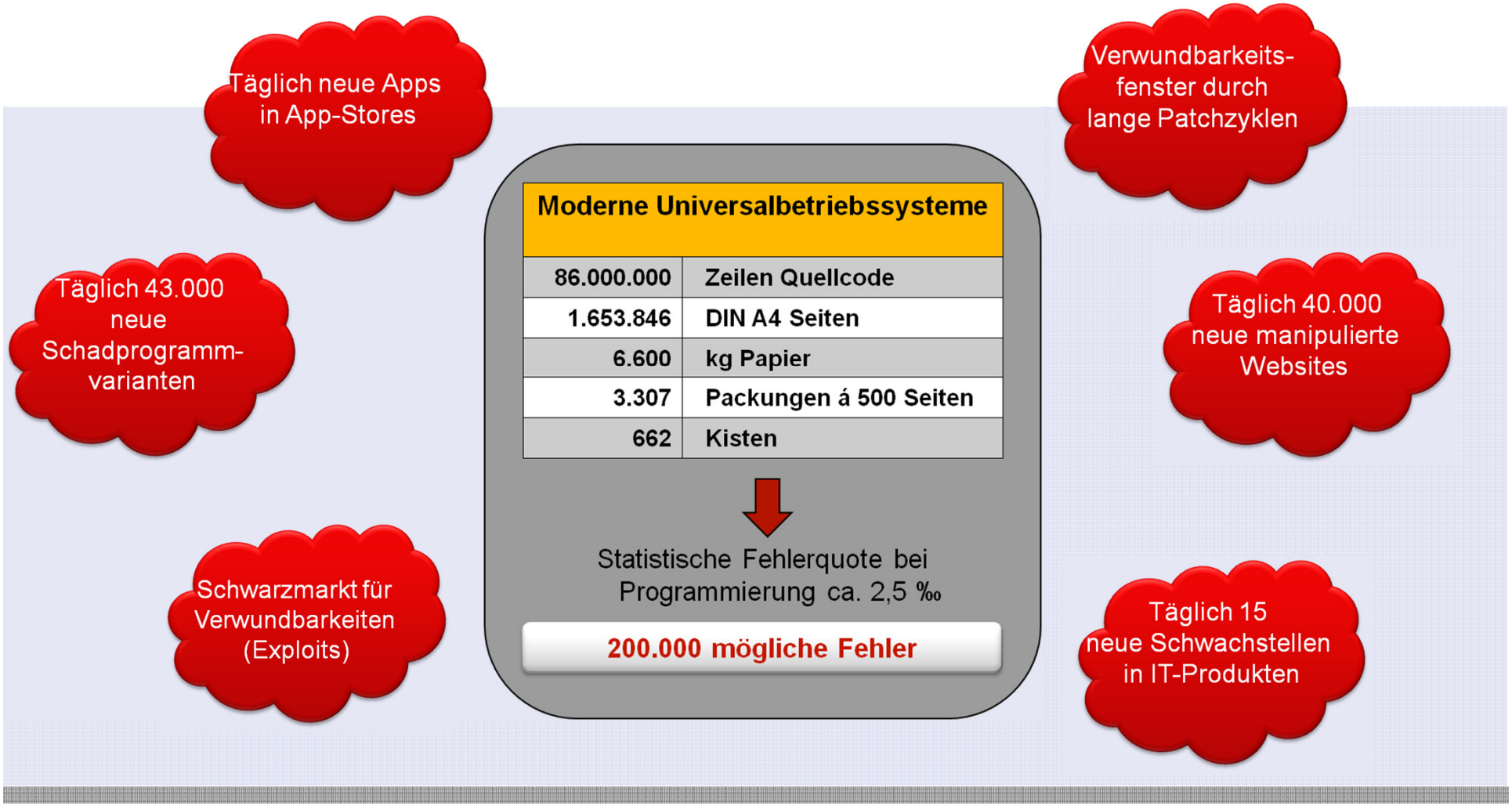
Cyber-Sicherheitsstrategie
Stand und nächste Schritte

Fachkonferenz : Mit Sicherheit Internet
Münchner Kreis
29. März 2012, München

Martin Schallbruch
IT-Direktor im Bundesministerium des Innern

Bundesministerium des Innern

Die Ursachen für Cyber-Unsicherheit. Komplexität und Verwundbarkeit der IT.



Bundesministerium des Innern

Cyber-Angriffe. Der Aufwand geht mit dem Ziel und den Motiven des Angreifers einher.

Ungezielte Angriffe

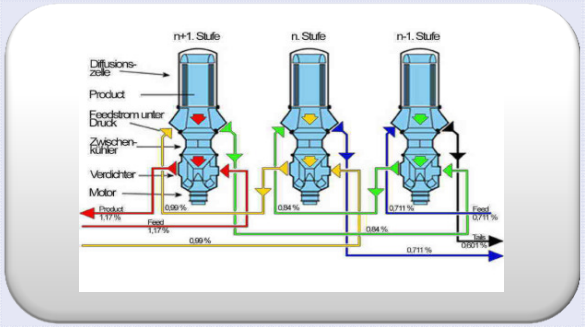
- Sabotage, Betrug, etc.
- Unspezifische Zielgruppen
- **SPAM, Viren, Würmer, Trojaner, Drive-by-Downloads**

Gezielte Angriffe

- Spionage und Sabotage
- Spezielle Zielgruppen
- **Social-Engineering + Trojaner**

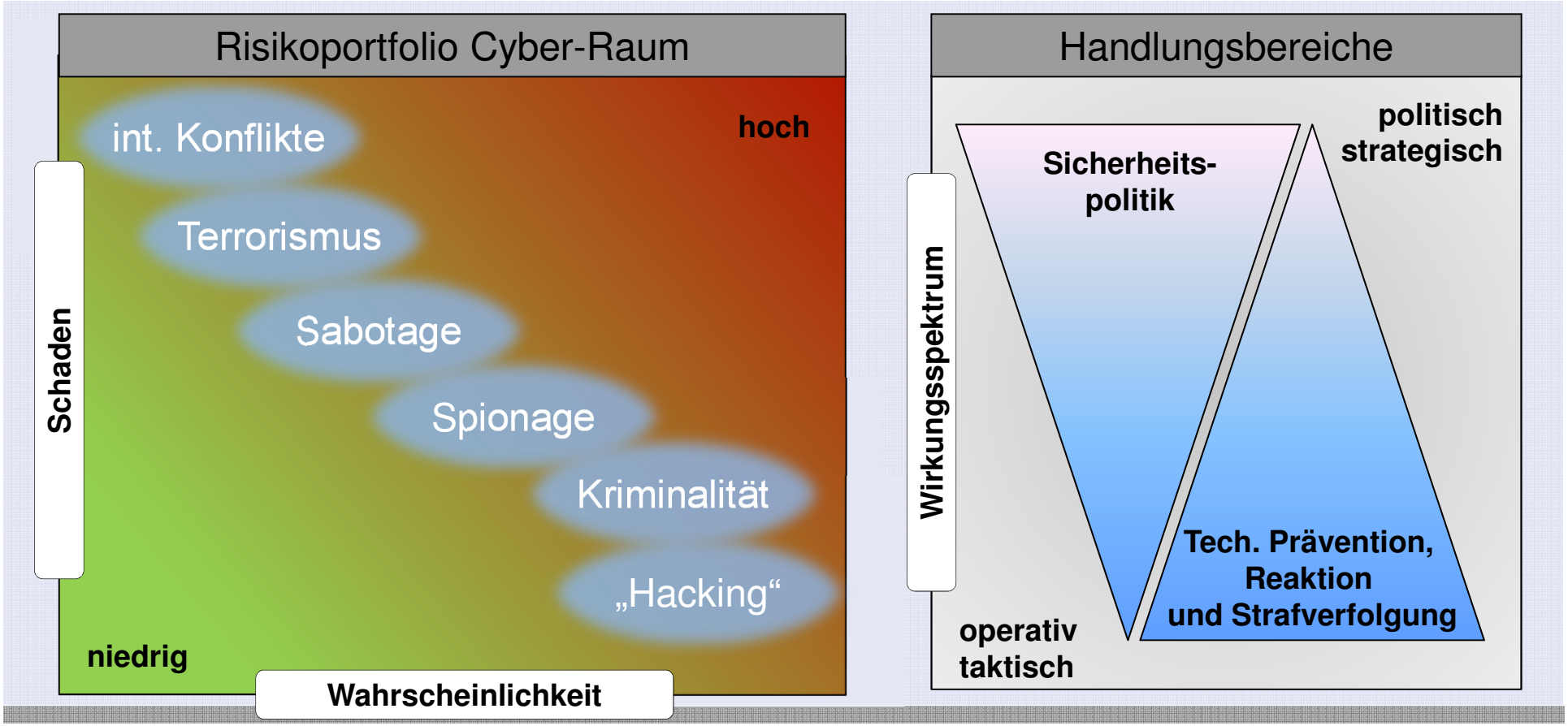
Skalpellartige Angriffe

- Sabotage spezieller IT-Systeme (und Infrastrukturen) mit großem Schadensausmaß
- Komplexe, langwierige Vorbereitung
- **Zero-Day-Verwundbarkeiten**
- **Fälschung von Zertifikaten**



Bundesministerium des Innern

Bedrohungslage im Cyber-Raum. Das Risikoportfolio erfordert individuelles Vorgehen.



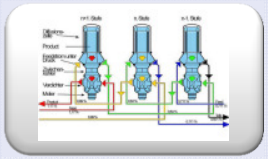
Bundesministerium des Innern

Schwerpunkt der Regierungsarbeit seit 2009: Cyber- und IT-Sicherheit.

November 2009 — *Herbst 2010* — *Februar 2011*

IT-Sicherheit im Koalitionsvertrag

- Stärkung der IT-Sicherheit im öffentlichen und nicht-öffentlichen Bereich, insb. Schutz kritischer IT-Systeme
- Bündelung von Kompetenzen beim Bundes-CIO
- BSI als zentrale Cyber-Sicherheitsbehörde weiter ausbauen
- Unbilliger Abwälzung von IT-Risiken auf die Endanwender vorbeugen



„Stuxnet“

„Duqu“

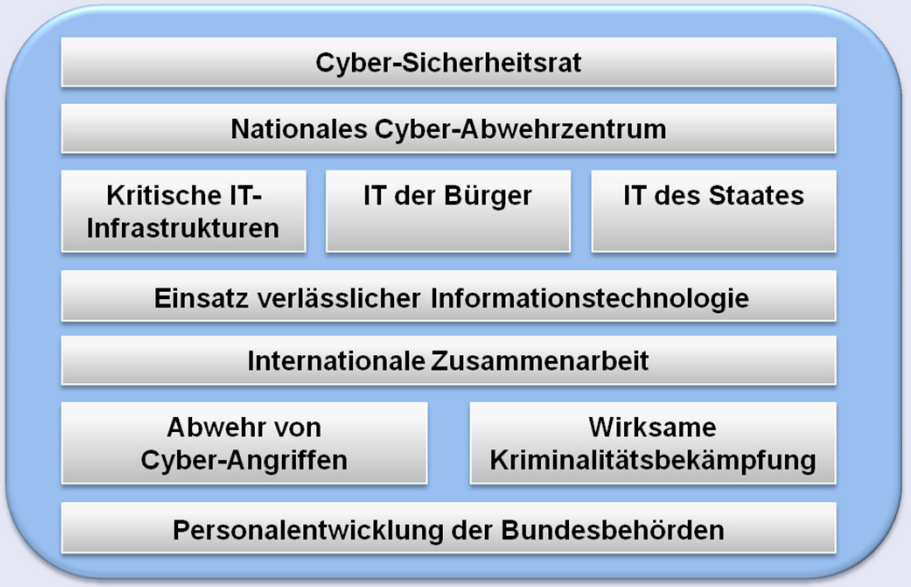
Cyber-Sicherheitsstrategie

Bundesministerium des Innern

Die Cyber-Sicherheitsstrategie von 2011. Strategische Ziele und Maßnahmen.

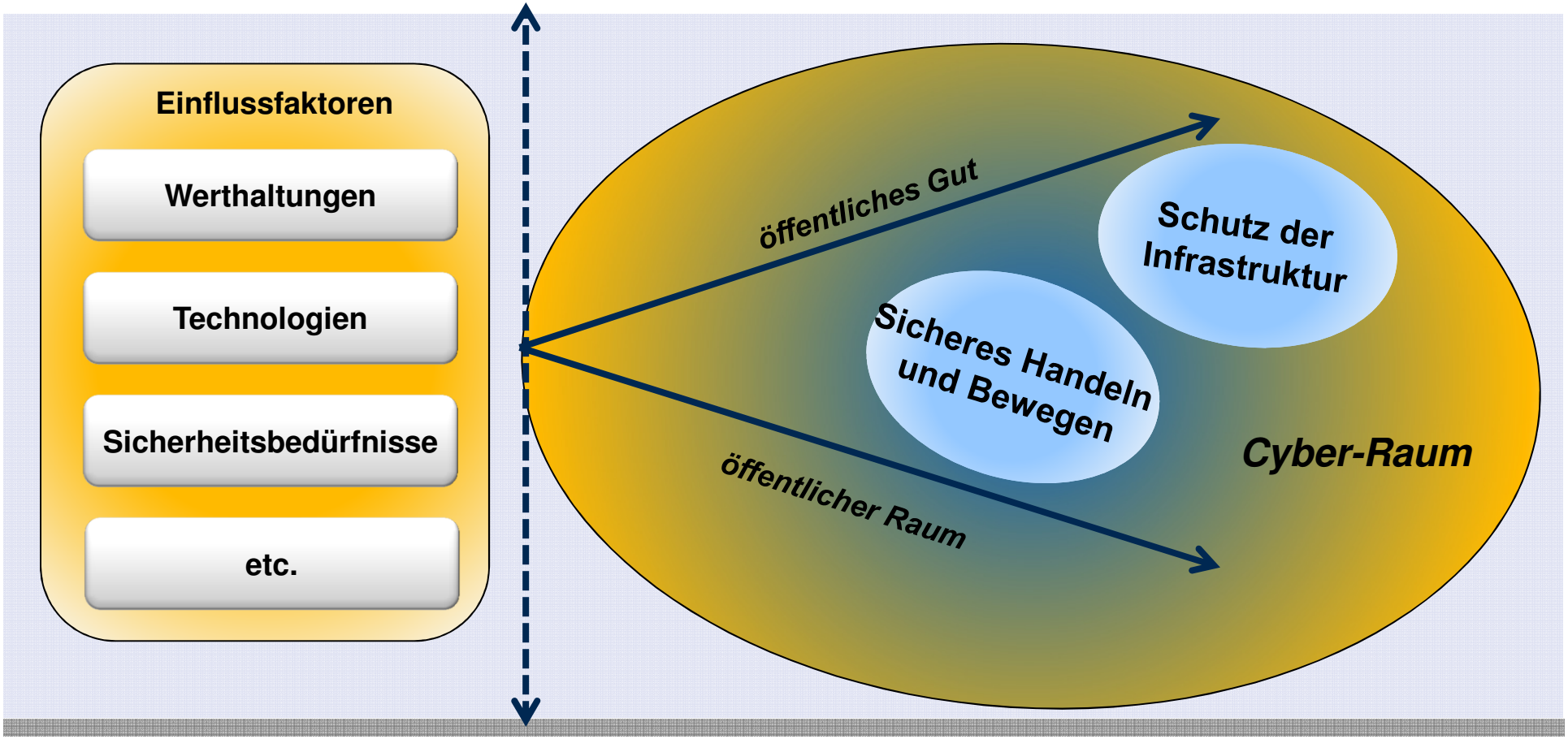
Beschluss des Bundeskabinetts am 23. Februar 2011

„ Ziel der am 23.02.2011 beschlossenen Cyber-Sicherheitsstrategie für Deutschland ist es, Cyber-Sicherheit auf einem der Bedeutung und der Schutzwürdigkeit der vernetzen Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen.“



Bundesministerium des Innern

Sicherheit und Cyber-Raum. Staatliches Handeln wirkt mehrdimensional.



Kritische Informationsinfrastrukturen

Aktueller Stand

- Umsetzungsplan UP KRITIS
- Kooperation mit Betreibern in 4 Arbeitsgruppen
- Weiterer Aufbau von Single Points of Contacts (SPOCS)

Nächste Schritte

- Organisatorische/inhaltliche Weiterentwicklung des UPK
- Strategische Ausweitung des Teilnehmerkreises UPK
- Definition sektorspezifischer Mindestsicherheitsanforderungen
- Festigung/Ausbau von Melde- und Alarmierungsprozessen
- Evaluierung der aufsichts-rechtlichen Grundlagen

Bundesministerium des Innern

Stärkung der IT-Sicherheit in der öffentlichen Verwaltung

Aktueller Stand

- Umsetzungsplan BUND
- IT-Steuerung BUND
- IT-Sicherheitsmanagement
- BSI-Gesetz § 8
  - Mindestanforderungen
  - Zentrale Beschaffung von IT-Sicherheitsprodukten

Nationaler Plan zum Schutz der Informationsinfrastrukturen
Umsetzungsplan BUND

Nächste Schritte

- Ressortübergreifende Vereinheitlichung für IT-Sicherheit in Verwaltung
- Verankerung von IT-Grundschutz als Standard für Verwaltung
- Verzahnung von IT-Rat mit Cyber-Sicherheitsrat

IT-Planungsrat

Rat der IT-Beauftragten

Sichere IT-Systeme in Deutschland

De-Mail

Anti-Botnet
Beratungszentrum

Aktueller Stand

- Basissicherheitsinfrastrukturen De-Mail, nPA
- Bürger-CERT
- **BSI/BITKOM Allianz für Cyber-Sicherheit**
- Deutschland sicher im Netz
- BMWi Task Force „IT-Sicherheit in der Wirtschaft“
- Antibotnetz-Beratungszentrum

BÜRGERCERT
Ins Internet - mit Sicherheit

Nächste Schritte

- Mindestanforderungen an TK-Provider und Befugnisse zur Erkennung von Schadaktivitäten (SPAM/Botnetz-Schutz)
- Etablierung von Meldewegen für erkannte skalierende IT-Vorfälle
- Einführung Mindeststandard Nutzerinformation und Sicherheitswerkzeuge für Nutzer
- 24/7 Erreichbarkeit von Providern

Nationales Cyber-Abwehrzentrum

Nationales Cyber-Abwehrzentrum

Aktueller Stand

- Operativer Betrieb seit 1. April 2011
- Nukleus: BSI, BfV und BBK
- Vernetzung mit IT-Lagezentrum und IT-Krisenreaktionszentrum
- Anbindung der Sicherheitsbehörden
- Analyse von IT-Vorfällen
- Abstimmung von Handlungsempfehlungen

Nationales IT-Lagezentrum BSI

CERT Bund

Nächste Schritte

- Erweiterung um aufsichtsführende Behörden bei KRITIS-Sektoren
- Internationale Vernetzung

Bundesministerium des Innern

Nationale Cyber-Sicherheitsrat (auf Staatssekretärsebene)

Aktueller Stand

- Konstituierung in 05/11, 2. Sitzung in 11/11, 3. Sitzung 05/12
- Mitglieder: BK, BMI, AA, BMWi, BMF, BMJ, BMBF, BMVg, 2 Ländervertreter
- Assoziierte Wirtschaftsvertreter: BDI, DIHK, BITKOM und Energiebranche
- Schwerpunktarbeit bisher:
  - Kritische Infrastrukturen
  - Cyber-Außenpolitik

Nächste Schritte

- 2-3 Sitzungen pro Jahr
- Kontinuierliche Identifikation und Bewertung struktureller Probleme und Herausforderungen auf politisch-strategischer Ebene
- Bewertung und Empfehlungen politischer Handlungs-möglichkeiten

Bundesministerium des Innern

Effektives Zusammenwirken in Europa und weltweit

Aktueller Stand

- EU Aktionsplan zum Schutz kritischer Informationsinfrastrukturen
- Meridian-Prozess seit 2005
- Kooperation BSI, BKA mit FBI: "DNSChanger„
- EU-US Cyber-Security
- Norms of State Behavior/VSBM
  - Bilateral insb. USA
  - Quad (DEU, FRA, UK, U.S.)
  - G8 (Deauville Mai 2011)
  - Vereinte Nationen
  - OSZE

Nächste Schritte

- Meridian Konferenz 2012 in DEU
- Bilaterale Konsultationen u.a. mit RUS u. CHN
- Mitarbeit in VN-Expertengruppe zu Norms of State Behavior
- Ggf. Mitarbeit in OSZE-AG zur Entwicklung von VSBM
- Zuständigkeitszuweisung für Cyber-Crime an das BKA
- Begleitung der NATO-Aktivitäten zur Umsetzung der Cyber Defence Policy aus 2011

Bundesministerium des Innern

Für Fragen und Diskussion nach der Veranstaltung: Kontaktinformationen.

Martin Schallbruch
IT-Direktor im
Bundesministerium des Innern

Alt-Moabit 101D
10559 Berlin

E-Mail:
martin.schallbruch@bmi.bund.de